Notice of Allowability	Application No.	Applicant(s)	
	09/304,444	BURNS ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *04/13/06*.

2. ☒ The allowed claim(s) is/are *1,3-8,11,12 and 15-19*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 04/13/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

HOSUK SONG
PRIMARY EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dave Thompson on 6/13/06.

The application has been amended as follows:

Replace claim 1 with the claim below:

1. (Currently Amended) A system for porting user data from one computer to another, comprising:
a memory device configured to store the user data and a public key; and
a smart card associated with a user that alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when the smart card is absent;
wherein the public key is sent from the memory device to the smart card, wherein the smart card contains a private key, and wherein access to the user data in the memory device is enabled upon verification that the public key and the private key are associated as a public/private key pair such that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key; and
wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 5 with the claim below:

5. (Currently Amended) A profile carrier comprising:
a smart card to store a passcode and a private key from a private/public key pair; and
a memory device to store a user profile and a public key from the private/public key pair;
wherein, when the smart card and the memory device are interfaced with a common computing unit, the smart card is configured to permit use of the private key following validation of a user-entered passcode with the stored passcode and to authenticate, using the private key, the public

key sent to the smart card from the memory device, wherein the authentication requires that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key;
wherein the profile carrier is configured to permit access to the user profile stored on the memory device upon successful authentication of the public key at the smart card; and
wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 7 with the claim below:

7. (Currently Amended) A computer system, comprising:
a computer having an interface; and
a profile carrier adapted to use the interface, the profile carrier comprising a smart card associated with a user, the smart card containing a private key, and a memory device having data memory to store a user's profile, the memory device storing a public key associated with the private key, wherein the smart card alternately enables access to the user's profile when present and disables access to the user's profile when absent;
wherein the system is configured to send the public key from the memory device to the smart card, and wherein access to the user data in the memory device is enabled upon verification that the public key and the private key are associated as a public/private key pair such that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key; and
wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 11 with the claim below:
11. (Currently Amended) A computer system, comprising:
a computer having a memory drive and a card reader;
a portable profile carrier to port a user's profile for configuration of the computer, the profile carrier comprising:

(a) an integrated circuit (IC) card associated with the user that can be interfaced with the computer via the card reader; and

(b) a memory device to store the user's profile, the memory device being interfaced with the computer via the memory drive, the IC card enabling access to the user data on the memory device;

wherein when the profile carrier is interfaced with the computer, the user's profile is accessible to configure the computer;
wherein the IC card stores a passcode and a private key of a public/private key pair;
wherein the memory device stores a public key of the public/private key pair; and
wherein the IC card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key

sent from the memory device to the IC card, wherein the authentication requires confirmation that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key; and
wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 15 with the claim below:
15. (Currently Amended) A method for porting a user profile for a computer, comprising:
storing a user profile in memory of a smart card secured profile carrier, the smart card secured profile carrier having a smart card that selectively enables access to the user profile in the memory;
interfacing the smart card secured profile carrier with the computer;
sending a public key, stored in the memory, to the smart card;
verifying that a private key, stored on the smart card, is associated with the public key, received from the memory, as a public/private key pair, wherein the association requires that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key, and wherein the public key is stored within the memory and sent to the smart card to facilitate the verifying;
reading the user profile from the memory, upon a successful verification, for use in configuring the computer; and
passing an encryption key, from the smart card and to the memory device, for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 17 with the claim below:
17. (Currently Amended) A method comprising:
storing user data and a public key on a portable memory device;
storing a private key on a smart card;
interfacing the smart card and the portable memory device with a computer;
sending the public key to the smart card;
verifying compatibility of the public key and the private key, wherein the verification requires that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key;
passing an encryption key, from the smart card to the memory device, for decryption of data read from the memory device, and for encryption of data to be stored on the memory device; and
allowing, in response to the verified compatibility, access to the user data on the portable memory device.

Replace claim 18 with the claim below:

18. (Currently Amended) A method comprising:
storing user data in a portable memory device;
storing a public key in the memory device;

storing a private key on the smart card, the card-resident key corresponding to the device-resident key;
storing a passcode on the smart card;
interfacing the smart card with a computer;
interfacing the portable memory device with the computer;
receiving a user-entered passcode;
permitting use of the private key following validation of the user-entered passcode with the passcode stored on the smart card;
passing the public key from the memory device to the smart card;
authenticating, at the smart card, the public key using the private key, thereby confirming that the public key and the private key are associated as a public/private key pair, such that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key;
permitting access to the user data stored in the memory device upon successful authentication of the public key; and
passing an encryption key, from the smart card and to the memory device, for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Replace claim 19 with the claim below:

19. (Currently Amended) In a system having a computer and a smart card secured profile carrier, the smart card secured profile carrier having memory to store a user profile and a smart card separate from the memory, computer-readable media resident on the profile carrier having executable instructions comprising:

receiving a user-supplied passcode from the computer;
authenticating the user-supplied passcode with a passcode stored on the smart card;
enabling access to a private key on the smart card upon successful authentication of the user-supplied passcode;
sending a public key from the memory to the smart card;
authenticating the public key using the private key, thereby confirming that the public key and the private key are a public/private key pair, such that the public and private keys are components of an asymmetric cryptographic system whereby data encrypted by the public key is decrypted by the private key;
enabling access to the user profile in the memory upon successful authentication of the public key; and
passing an encryption key, from the smart card and to the memory device, for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK
Friday, June 23, 2006

HOSUK SONG
PRIMARY EXAMINER